A special basis for the Leech lattice

Voskuil, Harm

Published in:
Proceedings of the Koninklijke Nederlandse Akademie van Wetenschappen. Series A:Mathematical Sciences

DOI:
10.1016/S1385-7258(87)80009-4

Publication date:
1987

A special basis for the Leech lattice

by Harm Voskuil

Mathematisch Instituut, Rijksuniversiteit Groningen, Postbus 800, 9700 AV Groningen, the Netherlands

Communicated by Prof. T.A. Springer at the meeting of September 29, 1986

1. INTRODUCTION

The Leech lattice is the unique even unimodular lattice in $\mathbb{R}^{24}$ having vectors of minimum squared norm 4. There are no such lattices in smaller dimensions. Let R be the set of minimum norm vectors of the Leech lattice Λ. We shall construct a basis $\alpha_1, \ldots, \alpha_{24}$ of Λ consisting of elements of R such that:

$$\forall(\alpha \in R)\ \alpha = \sum n_i \alpha_i \Rightarrow (\forall n_i \geqq 0) \vee (\forall n_i \leqq 0).$$

This property is similar to the condition that defines a basis for a root system, called a basis of simple roots in [2].

First a short description of the extended binary Golay code is given. Some well-known facts will be stated and properties that are useful for the sequel will be proved. Then we use this code to construct the Leech lattice and the special basis mentioned above. Finally we will compare this special basis with a base of root systems.

We thank W.H. Hesselink for his encouragement during the preparation of this paper.

2. THE GOLAY CODE

The extended binary Golay code C is a 12 dimensional linear code in $\mathbb{F}_2^{24}$, with minimum weight 8. The weight of a vector x is defined as $w(x) = \text{card}\ \{i | x_i \neq 0\}$. The only weights appearing in this code are 0, 8, 12, 16 and 24.

We define the vectors $c_0, \ldots, c_{11}$ of a basis of C by their coordinates, as listed in table 1. This basis can easily be deduced from the basis of C given in [3]. The ordering of the coördinates is not the same as the one given there. In particular there is an irregularity at the 13^{th} and 14^{th} coördinate. Those columns have been interchanged here in order to simplify the construction of a basis of the Leech lattice.

Table 1. The basis of C.

0	1	1	1	1	1	1	1	1	1	1	0	1	0	0	0	0	0	0	0	0	0	0	c_0
1	1	0	0	0	1	0	1	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	c_1
1	1	1	0	0	0	1	0	1	1	0	1	0	0	1	0	0	0	0	0	0	0	0	c_2
1	1	1	1	0	0	0	1	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	c_3
1	0	1	1	1	0	0	0	1	0	1	1	0	0	0	0	1	0	0	0	0	0	0	c_4
1	1	0	1	1	1	0	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	c_5
1	1	1	0	1	1	1	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	c_6
1	0	1	1	0	1	1	1	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	c_7
1	1	0	1	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	c_8
1	0	1	0	1	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	c_9
1	0	0	1	0	1	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	1	c_{10}
1	0	0	0	1	0	1	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	c_{11}

From table 1 it follows that $w(c_0)=12$ and $w(c_i)=8$, $i=1\cdots 11$. For convenience $\mathbb{F}_2^{24}$ will sometimes be identified with the power set of $\{1\cdots 24\}$. In particular, for $x\in\mathbb{F}^{24}$ the notation $i\in x$ will mean $x_i=1$. Also for a subset V of $\{1\cdots 24\}$ the notation $V\in C$ means that there is a vector $Y\in C$ with $\{i\,|\,Y_i\neq 0\}=V$.

DEFINITION. A vector of weight 8 in C is called an octad. A vector of weight 12 in C is called a dodecad.

LEMMA 1. a) An octad has exactly 2, 4 or 6 coördinates in common with a dodecad.

b) A vector in C which has exactly 2 coördinates not in a dodecad is an octad.

c) A vector in C which has exactly 4 coördinates not in a dodecad x is either a dodecad or an octad. If it is a dodecad than its sum with x is an octad, and conversely.

PROOF. a) Since the sum y of an octad and a dodecad is in C, it must have weight 0, 8, 12, 16 or 24. On the other hand we have $12-8\leqq w(y)\leqq 12+8$. So $w(y)$ is 8, 12 or 16 and the octad and the dodecad have 2, 4 or 6 non-zero coördinates in common.

b) If a vector y in C has 2 coördinates not in a dodecad x, it has at least weight 8 and then $w(x+y)=8$. If $w(y)>8$ then $0<w(x+y)<8$, which is impossible. So y must be an octad.

c) If a vector y has exactly 4 coördinates not in a dodecad x then $4\leqq$ $\leqq w(x+y)\leqq 16$. From $w(y)\geqq 8$ it follows that $w(x+y)\neq 16$. So $w(y)=8$ or $w(y)=12$, since $y\in C$. The last statement follows from: $w(y)=8\Rightarrow w(x+y)=12$.

LEMMA 2. There is a basis $d_0 \cdots d_{11}$ of C, obtained from $c_0, \ldots, c_{11}$ by a permutation of the coördinates, such that d_0 is the complement of c_0 and $d_1 \cdots d_{11}$ are octads.

PROOF. We will give an explicit construction of such a basis. The vector d_0 is known. The vectors d_i, $i = 1 \cdots 11$ are the sum of c_0 and the octads c_j of which the i^{th} coördinate in A is 1. Here $A = (\alpha_{ij})$ is given by $\alpha_{ij} = (c_i)_{j+1}$, $i, j = 1 \cdots 11$. So for example $d_1 = c_0 + c_1 + c_2 + c_3 + c_5 + c_6 + c_8$. The i^{th} column of A contains six times 1, so the $i+1^{\text{th}}$ coördinate of d_i is 1. Since two rows of A have three non-zero coördinates in common, two columns of A have also three non-zero coördinates in common, so the other coördinates in A of d_i, $i \neq 0$, are zero. This basis $d_0 \cdots d_{11}$ is given by the rows of the following 12×24 matrix:

$$\begin{pmatrix} d_0 \\ \vdots \\ d_{11} \end{pmatrix} = \begin{pmatrix} & 1 & 0 & u' \\ I_{12} & & & \\ & b & u & B \end{pmatrix}$$

where $u' = (1, 1, 1, \ldots, 1)$ and $(b\ B)$ is a cyclic 11×11 matrix with first row: 11101101000. It is easy to see that this basis can be changed into the basis $c_0 \cdots c_{11}$ by a permutation of the coördinates.

THEOREM 1. The octads in C form a Steiner system $S(5, 8, 24)$.

PROOF. The statement means that every five different coördinates define exactly one octad: For every system of pairwise different coördinates $i_1 \cdots i_5 \in \in \{1 \cdots 24\} \exists (x \in C)\ x_{i_1} = \cdots = x_{i_5} = 1 \wedge w(x) = 8$. This is a well-known fact ([3], p. 99), but we need the explicit form of the octads for the construction of the basis below. Since the minimum weight of a non-zero vector in C is 8, two different octads can have at most 4 non-zero coördinates in common. So 5 coördinates can be in at most one octad. To prove that they are in exactly one octad, we will count the octads. It is obvious that the number of octads in a Steiner system $S(5, 8, 24)$ is $|S(5, 8, 24)| = \binom{24}{5}/\binom{8}{5} = 759$.

There are $2.11 + 2.\binom{11}{2}$ octads having two coördinates not in c_0. They are c_i, $c_i + c_0$, $i = 1 \cdots 11$ and $c_i + c_j$, $c_i + c_j + c_0$, $1 \leqq i < j \leqq 11$, they are octads by lemma 1 (b). It follows from lemma 1 (c) that either $c_i + c_j + c_\kappa$ or $c_i + c_j + + c_\kappa + c_0$, $1 \leqq i < j < \kappa \leqq 11$ and either $c_i + c_j + c_\kappa + c_l$ or $c_i + c_j + c_\kappa + c_l + c_0$, $1 \leqq i < j < \kappa < l \leqq 11$ are octads, since they have 4 coördinates not in c_0. Thus we find $\binom{11}{3} + \binom{11}{4}$ octads. Octads having 6 coördinates not in c_0 are found by using the basis constructed in lemma 2. There are $2.11 + 2.\binom{11}{2}$ such octads, they are of the form d_i, $d_i + d_0$, $i = 1 \cdots 11$ and $d_i + d_j$, $d_i + d_j + d_0$, $1 \leqq i < j \leqq 11$. In total we have now $4.11 + 4.\binom{11}{2} + \binom{11}{3} + \binom{11}{4} = 759$ octads.

DEFINITION. For a vector x in C we define $\max(x) = \max\{i \mid x_i = 1\}$. An octad is called *decomposable* if there are octads $y, z \in C$ such that $x = y + z$, $\max(x) > > \max(y)$ and $\max(y) \notin x$.

LEMMA 3. The indecomposable octads generate C.

PROOF. The octads generate C, since the octads c_1+c_0, c_i, $i=1\cdots 11$ form a basis of C. Now we only have to show that every octad is a sum of indecomposable octads.

Suppose there is an octad x which is not the sum of indecomposable octads. This octad x cannot be indecomposable. At least one of the octads in the decomposition of x is not a sum of indecomposable octads, otherwise x would be a sum of indecomposable octads. So if we decompose an octad which is not a sum of indecomposable octads and do this in every decomposition again, then we get an infinite series of decompositions. Since there are only finitely many octads: there must be at least one octad which is not a sum of indecomposable octads, that occurs more than once in this series. Let us choose such an octad and call it z. Suppose the decomposition of z is $z=a_1+b_1$ and b_1 is not a sum of indecomposable octads. We get an infinite series of decompositions $b_i=$ $=b_{i+1}+a_{i+1}$ and $b_n=z$ for some $n\geqq 1$. From $z=(\sum_{i=1}^{n} a_i)+z$ it follows that $a_1=\sum_{i=2}^{n} a_i$. Since $\max(b_i)=\max(z)$, $i=1\cdots n$ we get by induction that $\max\{\max(a_i)|i=2\cdots n\}\notin b_1$ and $\max\{\max(a_i)|i=2\cdots n\}=\max(\sum_{i=2}^{n} a_i)=$ $=\max(a_1)$. So $\max(a_1)\notin b_1$ and $z=a_1+b_1$ is not a decomposition since $\max(b_1)=\max(z)$.

THEOREM 2. There are exactly 12 indecomposable octads in C. They form a basis of C. See table 2.

Table 2. The indecomposable octads in C.

1	1	0	0	0	1	0	1	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	c_1
1	0	1	1	1	0	1	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	c_0+c_1
0	1	0	1	1	0	0	0	1	0	0	1	1	1	1	0	0	0	0	0	0	0	0	$c_0+c_1+c_2$
0	1	1	0	1	1	0	0	0	1	0	0	0	1	1	1	0	0	0	0	0	0	0	$c_0+c_2+c_3$
0	0	0	1	0	0	0	1	0	1	0	0	1	1	1	1	1	0	0	0	0	0	0	$c_0+c_1+c_2+c_3+c_4$
0	0	0	0	1	0	0	0	1	0	1	0	0	1	1	1	1	1	0	0	0	0	0	$c_0+c_2+c_3+c_4+c_5$
0	0	0	0	0	1	0	0	0	1	0	1	0	1	0	1	1	1	1	0	0	0	0	$c_0+c_3+c_4+c_5+c_6$
0	0	0	0	1	0	0	1	0	0	0	0	1	0	0	1	1	1	1	1	0	0	0	$c_1+c_3+c_4+c_5+c_6+c_7$
0	0	0	0	0	1	0	0	1	0	0	0	0	0	1	0	1	1	1	1	1	0	0	$c_2+c_4+c_5+c_6+c_7+c_8$
0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	1	0	1	1	1	1	1	0	$c_3+c_5+c_6+c_7+c_8+c_9$
0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	1	0	1	1	1	1	1	$c_4+c_6+c_7+c_8+c_9+c_{10}$
0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	1	0	1	1	1	1	$c_5+c_7+c_8+c_9+c_{10}+c_{11}$

PROOF. From lemma 3 we know that the indecomposable octads generate C, so we only have to prove that there are at most 12 indecomposable octads.

First we look at octads x that are the sum of less than 4 octads c_i $i\neq 0$, and possibly c_0. Let us choose such an octad x and an octad c_i, $i\neq 0$, that does not contribute to x. From the proof of theorem 1, we know that $y=x+c_i$ or $x+c_i+c_0$ is again an octad, since y is the sum of at most 4 octads c_j, $j\neq 0$, and possibly c_0. If $\max(c_i)$ or $\max(c_i+c_0)$ is smaller than $\max(x)$ and not in x,

we can use the following decomposition: $x=c_i+(x+c_i)$ or $x=(c_i+c_0)+$ $+(x+c_i+c_0)$. This means that when m is the largest index of the octads c_j of which x is the sum, we have to choose an octad c_i, $0<i<m$, such that c_i does not contribute to x. In the case c_0 contributes to x we need an $i\neq 1$, if we have to use the decomposition with c_i+c_0.

Such an octad c_i, $i\neq 0$, can not be found if x is the sum of c_j's with successive indices starting with c_1, or also starting with c_2 when c_0 contributes to x and we have to use the decomposition with (c_i+c_0). This gives us the following list of vectors that are the sum of less than 4 octads c_i, $i\neq 0$, that might be indecomposable octads: c_1, c_1+c_0, c_1+c_2, $c_1+c_2+c_0$, $c_2+c_3+c_0$, $c_1+c_2+c_3$, $c_1+c_2+c_3+c_0$ and $c_2+c_3+c_4+c_0$. Since $c_1+c_2+c_3$ and $c_2+c_3+c_4$ are octads it follows from lemma 1 (b) that $c_1+c_2+c_3+c_0$ and $c_2+c_3+c_4+c_0$ are not octads. The other vectors in the list are octads. We can use the following decompositions:

$$c_0+c_2=(c_1+c_2+c_0)+c_1$$

$$c_1+c_2=(c_2+c_0)+(c_1+c_0)$$

$$c_1+c_2+c_3=(c_2+c_3+c_0)+(c_1+c_0).$$

So we have not given a decomposition for the octads c_1, c_1+c_0, $c_1+c_2+c_0$ and $c_2+c_3+c_0$.

If the octad x is the sum of 4, 5 or 6 octads c_i, $i\neq 0$, and possibly c_0 we need another way to construct a decomposition. In this case we take the 3 octads c_j, c_κ and c_l, which contribute to x and have the largest indices. Furthermore we choose an octad c_i, $i\neq 0$, such that $\max(x+c_j+c_\kappa+c_l)<\max(c_i)$ and $\max(c_i)<\max(x)$. It is obvious that $\max(c_i)\notin x$. If such an c_i exists then either $c_i+c_j+c_\kappa+c_l$ or $c_i+c_j+c_\kappa+c_l+c_0$ is an octad.

Let us call this octad y. Because x and y have at least 3 coördinates in common, they must have 4 coördinates in common. So $z=y+x$ is also an octad. From the fact that x is the sum of at least 4 octads and that we only used 3 of them to construct y, it follows that $i\neq 1$ and $\max(z)\neq\max(c_0)$ and $\max(z)\notin x$. Now we have the decomposition $x=y+z$, where $\max(z)=\max(c_i)$ and $\max(c_i)\notin x$.

The octads we have not given a decomposition of now, are those in which the last 4 coördinates are successive. Our construction of a decomposition certainly cannot work if the last 5 coördinates are successive. Let γ_{11} be the octad defined by the 5 coördinates $20\cdots 24$. Our basis of C is such that $\gamma_{11}=c_{11}+c_{10}+c_9+c_8+c_7+c_5$. From the fact that the matrix A in our description of the basis of C is cyclic, it follows that the only other octads that have 5 successive last coördinates and are the sum of 5 or 6 octads c_i, $i\neq 0$, are the following:

$$\gamma_{10}=c_{10}+c_9+c_8+c_7+c_6+c_4$$

$$\gamma_9=c_9+c_8+c_7+c_6+c_5+c_3$$

$$\gamma_8 = c_8 + c_7 + c_6 + c_5 + c_4 + c_2$$

$$\gamma_7 = c_7 + c_6 + c_5 + c_4 + c_3 + c_1$$

Let $x \notin \{\gamma_7, \ldots, \gamma_{11}\}$ and let the last 4 coördinates of x be successive. If there is a $\gamma_i \in \{\gamma_7, \ldots, \gamma_{11}\}$ such that $\max(x) = \max(\gamma_i)$ then we can use the following decomposition:

$$x = \gamma_i + (x + \gamma_i).$$

Otherwise $\max(x) < \max(c_7)$ and the 5 largest c_i that contribute to x cannot be successive. So we have not yet given a decomposition for the following octads:

$$c_1 + c_2 + c_3 + c_4 + c_0$$

$$c_2 + c_3 + c_4 + c_5 + c_0$$

$$c_3 + c_4 + c_5 + c_6 + c_0.$$

The vectors $c_0 + c_1 + c_3 + c_4 + c_5 + c_6$ and $c_1 + c_3 + c_4 + c_5 + c_6$ have 5 coördinates in common with γ_7, so they are not octads.

Now we have given a decomposition for all but 12 octads in C.

3. A BASIS FOR THE LEECH LATTICE

We will use a construction of the Leech lattice, cf. [1], based on the extended binary Golay code. In $\mathbb{R}^{24}$ we take a basis $b_1 \cdots b_{24}$ such that $(b_i, b_j) = \frac{1}{8}\,\delta_{ij}$. The Leech lattice Λ is defined by:

A vector $x = \sum x_i b_i$, $x_i \in C$ is in Λ iff.:

$$\exists(\gamma \in \{0,1\})\ \forall i\ x_i = \gamma \bmod 2$$

$$\sum x_i = 4\gamma \bmod 8$$

$$\forall(\alpha \in \{0,1,2,3\})\{i \mid x_i = \alpha \bmod 4\} \in C.$$

REMARK. We will use the following notation to describe the vectors $\sum n_i b_i = (n_1 \cdots n_{24})$. The zeros will be left out. When we do not care about the order of the coördinate we use a comma to separate them and when we do care we use a semicolon. Sometimes indices $i, j \cdots$ are used. Coördinates that contain the same number will be taken together. So e.g. (4^2) describes a vector $4b_i + 4b_j$, $i \neq j$, and $(-2^4, 2^3; 2)$ describes a vector with 4 coördinates $+2$ and 4 coördinates -2, such that the last non-zero coördinate is $+2$.

It follows from the definition of Λ, cf. [1], that the set R of the minimum norm vectors of Λ consists of vectors of the following form:

a) $\pm(4,4)$, $(-4,4)$

b) $\pm(2^8)$, $\pm(-2^2, 2^6)$, $(-2^4, 2^4)$; The non-zero coördinates form an octad in C

c) $\pm(3, 1^n, -1^{24-n-1})$; The plus ones are in C, so $n = 0$, 8, 12 or 16.

There are $2^2.\binom{24}{2} = 1104$ vectors of type a, $2^7.759 = 97152$ vectors of type b and $24.2^{12} = 98304$ vectors of type c in the Leech lattice Λ.

DEFINITIONS. A vector $z \in \mathbb{R}^{24}$ is called *regular* if $\forall(\alpha \in R)\ (z, \alpha) \neq 0$. If z is regular then we define $P_z = \{\alpha \in R | (z, \alpha) > 0\}$. We call a vector $a \in P_z$ *decomposable* if there are $\beta, \gamma \in P_2$ such that $\alpha = \beta + \gamma$, otherwise α is called *indecomposable*. The set of indecomposable vectors is denoted by S_z. A basis $\alpha_1 \cdots \alpha_{24}$ of Λ consisting of elements of R such that

$$\forall(\alpha \in R)\ \alpha = \sum n_i \alpha_i \Rightarrow (\forall n_i \geqq 0) \vee (\forall n_i \leqq 0)$$

is called a *simple basis*.

To find a simple basis of Λ one takes a regular vector z. It is well-known cf. [3], that the Leech lattice is generated by R, so it is generated by P_z. Since P_z is finite, it is generated by S_z. Therefore, if $|S_z| = 24$, then the 24 indecomposable vectors form a simple basis of Λ.

THEOREM 3. Let the extended binary Golay code C and the Leech lattice Λ be as above.

Let $z \in \mathbb{R}^{24}$ be a regular vector such that $(y, z) > 0$ for $y \in R$ and $y = \sum n_i b_i$ if $\sum y_i > 0$ or if $\sum y_i = 0$ and the last non-zero coördinate of y is positive. Then, with respect to this vector z, there are exactly 24 indecomposable vectors in the Leech lattice Λ, so they form a simple basis of Λ.

We fix a regular vector z as described in the statement of the theorem. The theorem will be proved by giving for every decomposable vector a decomposition. To improve readability the proof will be spread out over several lemmas.

LEMMA 4. The vectors in P_z are of the form $(-4; 4)$, $(4, 4)$, $(-3, 1^{23})$, $(-1^{11}, 3, 1^{12})$, $(1^{16}, 3, -1^7)$, $(1^{15}, -3, -1^8)$, (2^8), $(-2^2, 2^6)$ or $(-2^4, 2^3; 2)$.

PROOF. This is obvious.

LEMMA 5. There are at most 11 decomposable vectors of type $(-4, 4)$ and $(4, 4)$ in P_z.

PROOF. We can use the following decompositions:

$$(4_i, 4_j) = (2^4, 2_i, 2_j, -2^2) + (-2^4, 2_i, 2_j, 2^2);$$

Here the two vectors in the decomposition are based on one and the same octad. The signs are placed so as to make the last non-zero coördinate of the last vector positive.

$$(-4_i; 4_j) = (-4_i; 4_\kappa) + (-4_\kappa; 4_j),\ i < \kappa < j \text{ so } j \neq i+1$$

$$(-4_i; 4_{i+1}) = (-2^3, 2^3; -2_i; 2_{i+1}) + (2^3, -2^3; -2_i; 2_{i+1});$$

Here the two vectors in the decomposition are again based on one octad. The last coördinates must be i and $i+1$.

We can use the octads c_1; $c_1 + c_0$; $c_0 + c_2$; $c_j + c_{j+1}$, $j = 2 \cdots 10$. So we have not given a decomposition of the vectors $-4b_i + 4b_{i+1}$, $i \leqq i \leqq 11$.

Table 3. The indecomposable vectors in Λ.

−4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	α_1
4	−4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	α_2
0	0	−4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	α_3
0	0	0	−4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	α_4
0	0	0	0	−4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	α_5
0	0	0	0	0	−4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	α_6
0	0	0	0	0	0	−4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	α_7
0	0	0	0	0	0	0	−4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	α_8
0	0	0	0	0	0	0	0	−4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	α_9
0	0	0	0	0	0	0	0	0	−4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	α_{10}
0	0	0	0	0	0	0	0	0	0	−4	4	0	0	0	0	0	0	0	0	0	0	0	0	α_{11}
2	2	0	0	0	2	0	−2	−2	0	−2	−2	2	0	0	0	0	0	0	0	0	0	0	0	α_{12}
2	0	2	2	−2	0	−2	0	0	−2	0	0	−2	2	0	0	0	0	0	0	0	0	0	0	α_{13}
0	2	0	2	2	0	0	0	−2	0	0	−2	−2	−2	2	0	0	0	0	0	0	0	0	0	α_{14}
0	2	2	0	2	−2	0	0	0	−2	0	0	0	−2	−2	2	0	0	0	0	0	0	0	0	α_{15}
0	0	0	2	0	0	0	2	0	2	0	0	−2	−2	−2	−2	2	0	0	0	0	0	0	0	α_{16}
0	0	0	0	2	0	0	0	2	0	2	0	0	−2	−2	−2	−2	2	0	0	0	0	0	0	α_{17}
0	0	0	0	0	2	0	0	0	2	0	2	0	−2	0	−2	−2	−2	2	0	0	0	0	0	α_{18}
0	0	0	0	2	0	0	2	0	0	0	0	2	0	0	−2	−2	−2	−2	2	0	0	0	0	α_{19}
0	0	0	0	0	2	0	0	2	0	0	0	0	0	2	0	−2	−2	−2	−2	2	0	0	0	α_{20}
0	0	0	0	0	0	2	0	0	2	0	0	0	0	0	2	0	−2	−2	−2	−2	2	0	0	α_{21}
0	0	0	0	0	0	0	2	0	0	2	0	0	0	0	0	2	0	−2	−2	−2	−2	2	0	α_{22}
0	0	0	0	0	0	0	0	2	0	0	2	0	0	0	0	0	2	0	−2	−2	−2	−2	2	α_{23}
1	1	1	1	1	1	1	−1	1	1	−1	1	1	1	1	1	−1	1	−1	−1	−1	−1	−1	−3	α_{24}

LEMMA 6. All vectors in P_z of the form $(-3,1^{23})$, $(-1^{11},3,1^{12})$ and $(1^{16},3,-1^7)$ are decomposable.

PROOF. We can use the following decomposition:

$$(-3_i,1^{23})=(-3_i,1^{15},-1^8)+(2^8),$$

using an octad that does not contain coördinate i.

$$(1^{15},3_i,1_j,-1^7)=(1^{15},-1_i,-3_j,-1^7)+(4_i,4_j).$$

$$(-1^{10},3_j,-1_\kappa,1^{12})=(1^{14},1_j,-3_\kappa,-1^8)+(-2^4,2_j,2_\kappa,2^2);$$

Here the octad has been chosen by taking 5 coördinates in the dodecad $3-1^{11}$, including j. The coördinate κ is the last coördinate $\neq j$ the octad and the dodecad $3-1^{11}$ have in common. Recall that by lemma 1(a), the octad has 6 coördinates in common with the dodecad $3-1^{11}$. The last non-zero coördinate of the vector $(-2^4,2^4)$ is positive, since it is j,κ or in the dodecad 1^{12}. The sum of the dodecad 1^{12} and the octad is a vector of weight 16, so we can use the decomposition as described above.

LEMMA 7. There is at most one indecomposable vector of the form $(1^{15},-3,-1^8)$.

PROOF. Let x be a vector of the form $(1^{15},-3,-1^8)$. Let i be the index of -3 in x. In most cases we can use the following decomposition:

$$(-3_i,1^{14},1_j,-1^8)=(1_i,1^{14},-3_j,-1^8)+(-4_i;4_j),\ i<j.$$

If there is not a coördinate $j>i$ in the part 1^{15} of the vector x, then we must use another decomposition. We construct an octad by taking 4 coördinates in the octad -1^8 and one in its complement. The sum in $\mathbb{F}_2^{24}$ of this constructed octad and the vector of weight 16 is again a vector of weight 16. To get a valid decomposition with this octad in the form $(-2^4,2^4)$, we must make sure the last non-zero coördinate is positive. If the last coördinate of the vector x is -1, then we choose an octad containing the coördinates i and 24. As a decomposition we have:

$$(1^{15},-3_i,-1^7;-1_{24})=(1^{15},-1_i,-1^7;-3_{24})+(-2^3,2^3,-2_i;2_{24}).$$

If $i=24$, then we need an octad that has its last coördinate in the 1^{15} part of the vector x. Let j be the last $+1$ coördinate of x. For the construction of our octad we need 4 coördinates -1 on the left of j. First we assume that such coördinates exist. Together with j they define an octad.

If this octad does not contain coördinate 24, then we can use the following decomposition:

$$(1^{14},-1^8,1_j,-3_{24})=(1^{15},-1^7,-1_j;-3_{24})+(2^3,-2^4;2_j).$$

Suppose the constructed octad does contain the last coördinate. If there are at least 5 coördinates -1 on the left of j, then we can change one -1 coördi-

nate and construct a new octad. This octad can not contain the last coördinate, otherwise both constructed octads would have 5 coördinates in common. Now we can use the decomposition given above.

The vectors for which we have not given a decomposition have one of the following two series of last coördinates:

a) $\underline{1-1-1-1-1}\ -3, j=19$ and there are exactly 4 coördinates -1 on the left of j.

b) $\underline{-1-1-1-1-1}\ -3, j<19$ and there are less than 4 coördinates on the left of j.

In case a, we have only not given a decomposition if the octad constructed above contains the last coördinate. In this case the underlined coördinates are in the octad that is the sum of the constructed octad and the octad -1^8 that is in the vector x.

In case b, the octad -1^8 has 5 coördinates in common with the underlined octad of case a, so they must be the same.

This means that only case a or case b can occur and not both. Our basis of the Golay code is such that only case b. occurs. So we have exactly one vector of the form $(-1^8, 1^{15}, -3)$ left that could be indecomposable.

LEMMA 8. There are no indecomposable vectors in P_z of the form (2^8) and $(-2^2, 2^6)$.

PROOF. For these vectors we have the following decompositions:

$$(2^8) = (-2_i, -2_j, 2^6) + (4_i, 4_j).$$

$$(2^6, -2_i, -2_j) = (1^{14}, -3_i, 1_j) + (-1^8, 1_i, -3_j, 1^{14});$$

Here the three octads corresponding to $(2^6, -2^2)$ and -1^8 in both vectors have no coördinates in common.

LEMMA 9. There are at most 12 indecomposable vectors of the form $(-2^4, 2^3; 2)$ in P_z.

PROOF. Let x be a vector of the form $(-2^4, 2^3; 2)$. Let κ be the last non-zero coördinates of x. If x is not of the form $(2^3; -2^4; 2)$ then we can use the following decomposition:

$$(-2_i, 2_j, -2^3, 2^2; 2_\kappa) = (2_i, -2_j, -2^3, 2^2; 2_\kappa) + (-4_i, 4_j),\ i<j<\kappa.$$

In fact, then there are coördinates i and j in x, such that $x_i = -2$ and $x_j = 2$.

If x is of the form $(2^3; -2^4; 2)$, then we try a decomposition using two vectors y and z of the form $(-2^4, 2^3; 2)$ such that $x = y + z$. This means that the sum of the octads on which the vectors y and z are based is the octad corresponding to the vector x. Since the last non-zero coördinates of y and z have to be positive, we need an y which has a last non-zero coördinate κ, and an z which has a last non-zero coördinate $j<\kappa$, such that the corresponding coördi-

nate in x is zero. Such vectors y and z exist when the octad on which the vector x is based is decomposable. In theorem 2 we have proved that there are exactly 12 indecomposable octads. So we have not given a decomposition for 12 vectors of the form $(2^3; -2^4; 2)$.

In the lemmas 4 till 9 we have proved that there are at most 24 indecomposable vectors. So we have proved the theorem.

4. SOME REMARKS ABOUT THIS BASIS

We will compare the constructed basis of Λ with a basis of simple roots. A basis of simple roots is unique up to automorphisms, cf. [2]. In the following proposition we will prove that a simple basis of Λ is not unique up to automorphisms.

PROPOSITION 1. The group .0 of isometric automorphisms of Λ does not act transitively on the set of simple bases of the Leech lattice.

PROOF. We will construct another simple basis of Λ. Instead of taking another regular vector z we change the ordering of the coördinates of C. Let us permute the first and the second coördinate of the basis of C given above. With respect to the same regular vector z as used above we get 24 indecomposable vectors, since the decompositions given above are still valid mutatis mutandis. Let us call these 24 indecomposable vectors $\alpha_1' \cdots \alpha_{24}'$. If we now permute the first and second coördinate again these $\alpha_1' \cdots \alpha_{24}'$ are transformed into a simple basis $\alpha_1'' \cdots \alpha_{24}''$ of Λ. It is easy to see that $\alpha_1'' = -\alpha_1$, $\alpha_2'' = \alpha_1 + \alpha_2$ and $\alpha_i'' = \alpha_i$, $i = 3 \cdots 24$. The basis $\alpha_1'' \cdots \alpha_{24}''$ can not be transformed into the basis $\alpha_1 \cdots \alpha_{24}$, since $(\sum \alpha_i'', \sum \alpha_i'') \neq (\sum \alpha_i, \sum \alpha_i)$ as easily can be calculated. See table 3.

PROPOSITION 2. There exist regular vector z such that $|S_z| > 24$.

PROOF. Instead of taking another vector z, we permute the coördinates of C. Let us take a permutation of the first 12 coördinates of C, such that the twelfth coördinate of c_1 is zero. If we take z as above, then $|S_z| = 25$. The extra indecomposable vector is $-4b_{12} + 4b_{13}$, since we cannot use vectors based on the octad c_1 to decompose this vector as done in lemma 5. All other decompositions remain valid mutatis mutandis and there is no decomposition possible for the 25 vectors of which we have not given a decomposition.

If one permutes the 13^{th} and 14^{th} coördinate of C and uses a regular vector as above, then $|S_z| = 26$. Now one of the extra indecomposable vectors is again $-4b_{12} + 4b_{13}$. There are now 13 indecomposable octads in C, instead of the 12 of theorem 2. So there are 13 indecomposable vectors of type $(2^3, -2^4; 2)$ in Λ. All other decompositions are valid mutatis mutandis.

DEFINITION. For a vector $\alpha \in R$ we define its height as $ht(\alpha) = \sum n_i$, if $\alpha = \sum n_i \alpha_i$ and $\alpha_i \cdots \alpha_{24}$ is the simple basis of Λ constructed above. This defi-

nition of height is similar to the definition for a root system. It is well-known, cf. [2], that in an irreducible root system there is a unique root with maximal height relative to a simple basis. The following proposition shows that there is a unique vector of maximal height in Λ.

PROPOSITION 2. Let Λ and z be as above. There is a unique vector of maximal height. This vector is $(-3; 1^{23})$.

PROOF. We give a series of decompositions of vectors in P_z, showing that a vector of a certain form cannot have maximal height. The vectors on the left of the equality sign have a height smaller than those on the right side. The first vector in the decomposition is the one we can freely choose, so all vectors of this form have not maximal height. The decompositions that we use are:

$$\begin{aligned}
&(-2^4, 2^3; 2) && +(4^2) && = (-2^2, 2^6)\\
&(-2^2, 2^6) && +(4^2) && = (2^8)\\
&(2^8) && +(-3, -1^8, 1^{15}) && = (-3, 1^{23})\\
&(-4_i, 4) && +(4_i, 4) && = (4^2)\\
&(4^2) && +(-2^2, 2^6) && = (2^8)\\
&(-3, -1^8, 1^{15}) && +(2^8) && = (-3, 1^{23})\\
&(3_j, -1^7, 1^{16}) && +(-2_j, 2^6, -2_\kappa) && = (-3_\kappa, 1^{23})\\
&(-1^{11}, 3_j, 1^{12}) && +(2^6, -2^2) && = (-1^7, 3_j, 1^{16})
\end{aligned}$$

Here the vector $(2^6, -2^2)$ is based on an octad having 6 coördinates in common with the dodecad $-1^{11}\ 3_j$ and which does not contain coördinate j

$$(1; -3_i, 1^{22}) + (-4_1; 4_i) = (-3, 1^{23}).$$

REMARK. Note that we only have used the form of the vectors in P_z and not the explicit ordering of the coördinates in C.

REMARK. The height of this vector $(-3; 1^{23})$ is 149611. This can be seen by determining the vector $x \in \Lambda$ with $(x, \alpha) = 1$ for all $\alpha \in S_z$. The inner product of x with $(-3; 1^{23})$ equals 149611 and this must be the height of $(-3; 1^{23})$.

Let Δ be a basis of simple roots of a root system. A root system has the following property: If α is a positive root not contained in Δ, then there is a $\beta \in \Delta$ such that $\alpha - \beta$ is a positive root.

In the following proposition we will prove that our simple basis of Δ has no such properties.

PROPOSITION 3. There are $\alpha, \beta \in P_z$ such that there is no $\gamma \in P_z$ with $ht(\alpha) > ht(\gamma) > ht(\beta)$ and $ht(\alpha) > ht(\beta) + 1$.

PROOF. There are 196560 vectors in R, so there are 98280 vectors in P_z. From this and the fact that $ht[(-3; 1^{23})]$ is 149611 the proposition follows.

Table 4. The inner products (α_i, α_j).

(α_i, α_j)	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8	α_9	α_{10}	α_{11}	α_{12}	α_{13}	α_{14}	α_{15}	α_{16}	α_{17}	α_{18}	α_{19}	α_{20}	α_{21}	α_{22}	α_{23}	α_{24}
α_1	4	−2	0	0	0	0	0	0	0	0	0	0	−1	1	1	0	0	0	0	0	0	0	0	0
α_2	−2	4	−2	0	0	0	0	0	0	0	0	−1	1	−1	0	0	0	0	0	0	0	0	0	0
α_3	0	−2	4	−2	0	0	0	0	0	0	0	0	0	1	−1	1	0	0	0	0	0	0	0	0
α_4	0	0	−2	4	−2	0	0	0	0	0	0	0	−2	0	1	−1	1	0	1	0	0	0	0	0
α_5	0	0	0	−2	4	−2	0	0	0	0	0	1	1	−1	−2	0	−1	1	−1	1	0	0	0	0
α_6	0	0	0	0	−2	4	−2	0	0	0	0	−1	−1	0	1	0	0	−1	0	−1	1	0	0	0
α_7	0	0	0	0	0	−2	4	−2	0	0	0	−1	1	0	0	1	0	0	1	0	−1	1	0	1
α_8	0	0	0	0	0	0	−2	4	−2	0	0	0	0	−1	0	−1	1	0	−1	1	0	−1	1	1
α_9	0	0	0	0	0	0	0	−2	4	−2	0	1	−1	1	−1	1	−1	1	0	−1	1	0	−1	0
α_{10}	0	0	0	0	0	0	0	0	−2	4	−2	−1	1	0	1	−1	1	−1	0	0	−1	1	0	1
α_{11}	0	0	0	0	0	0	0	0	0	−2	4	0	0	−1	0	0	−1	1	0	0	0	−1	1	1
α_{12}	0	−1	0	0	1	−1	−1	0	1	−1	0	4	0	1	0	−1	−1	0	0	0	0	−1	−1	1
α_{13}	−1	1	0	−2	1	−1	1	0	−1	1	0	0	4	0	0	0	−1	−1	−1	0	−1	0	0	0
α_{14}	1	−1	1	0	−1	0	0	−1	1	0	−1	1	0	4	1	1	0	0	0	0	0	0	−1	0
α_{15}	1	0	−1	1	−2	1	0	0	−1	1	0	0	0	1	4	0	1	−1	0	−1	0	0	0	0
α_{16}	0	0	1	−1	0	0	1	−1	1	−1	0	−1	0	1	0	4	1	1	0	−1	0	1	0	−1
α_{17}	0	0	0	1	−1	0	0	1	−1	1	−1	−1	−1	0	1	1	4	1	1	0	−1	0	1	0
α_{18}	0	0	0	0	1	−1	0	0	1	−1	1	0	−1	0	−1	1	1	4	1	1	0	−1	0	0
α_{19}	0	0	0	1	−1	0	1	−1	0	0	0	0	−1	0	0	0	1	1	4	1	0	0	−1	0
α_{20}	0	0	0	0	1	−1	0	1	−1	0	0	0	0	0	−1	−1	0	1	1	4	1	0	0	1
α_{21}	0	0	0	0	0	1	−1	0	1	−1	0	0	−1	0	0	0	−1	0	0	1	4	1	0	1
α_{22}	0	0	0	0	0	0	1	−1	0	1	−1	−1	0	0	0	1	0	−1	0	0	1	4	1	0
α_{23}	0	0	0	0	0	0	0	1	−1	0	1	−1	0	−1	0	0	1	0	−1	0	0	1	4	1
α_{24}	0	0	0	0	0	0	−1	1	0	−1	1	1	0	0	0	−1	0	0	0	1	1	0	1	4

REMARK. The values of the inner products (α_i, α_j) that occur in our basis of Λ are $-2, -1, 0$ and $+1$. Furthermore $\forall i \exists j\ (\alpha_i, \alpha_j) \in \{1, -1\}$. This property follows from the fact that for all $\alpha \in R$ the reflection σ_α, defined by

$$\sigma_\alpha(y) = y - \frac{2(\alpha, y)}{(\alpha, \alpha)}$$

α is not in aut(Λ).

If $\exists i \forall j\ (\alpha_i, \alpha_j) \in \{2, 0, -2\}$ then $\sigma_{\alpha_i}(y)$ would be in Λ if $y \in \Lambda$. So the property is necessary for any basis of Λ consisting of minimum norm vectors. The inner products of our basis $\alpha_1 \cdots \alpha_{24}$ are shown in table 4.

REFERENCES

1. Conway, J.H. – Three lectures on exceptional groups. In "Finite Simple Groups" (ed. M.B. Powell & G. Higman), Academic Press 215–247, 1971.
2. Humphreys, J.E. – "Introduction to Lie algebras and representation theory". Springer-Verlag, 1972.
3. Van Lint, J.H. – "Coding Theorie". Springer Verlag, Lect. Notes in Mathematics **201**, 1971.